Rapports sur les accès pour Sarbanes-Oxley

Livre blanc de Bull Evidian

Apporter la preuve de la conformité à Sarbanes-Oxley

EVIDIAN
A Groupe Bull Company

Résumé

- La gestion raisonnée des identités et des accès
- Constitution de votre dossier pour vos auditeurs
- Exemple de chaînes SOX – risque, contrôle et test

© 2013 Evidian

Les informations contenues dans ce document reflètent l'opinion d'Evidian sur les questions abordées à la date de publication. En raison de l'évolution constante des conditions de marché auxquelles Evidian doit s'adapter, elles ne représentent cependant pas un engagement de la part d'Evidian qui ne peut garantir l'exactitude de ces informations passé la date de publication.

Ce document est fourni à des fins d'information uniquement. EVIDIAN NE FAIT AUCUNE GARANTIE IMPLICITE OU EXPLICITE DANS LE PRÉSENT DOCUMENT.

Les droits des propriétaires des marques cités dans cette publication sont reconnus.

EVIDIAN
A Groupe Bull Company

Table des matières

Introduction 4

La gestion raisonnée des identités et des accès 5

Cadre de référence de la loi Sarbanes-Oxley 6

Constitution de votre dossier pour vos auditeurs 7

Détermination des contrôles : le cycle de vie SOX 7
Que doit fournir un rapport sur la sécurité ? 7
Données exactes et non altérées 7
Reporting complet 8
Reporting adaptable 8
Environnement de production de rapports 9
Vérifiabilité 10
Rapport par actions ou par état 11

Exemple de chaînes SOX – risque, contrôle et test 12

Politique de sécurité du SI 14
Cycle de vie de la politique de sécurité 14
Authentification de l'utilisateur 15
Déployer une authentification unique dans toute l'entreprise 15
Forcer l'expiration du mot de passe 16
Gestion des autorisations d'accès de l'utilisateur 17
Suppression des comptes inactifs 17
Autorisations d'accès octroyées selon le profil 18
Auto-inscription 19
Reporting sur les incidents de sécurité 20
Eliminer les comptes par défaut 21
Cloisonnement des tâches 21
Exemple 21
Preuve d'accès aux ressources 22
Enregistrement des accès aux applications 22

Introduction

Régulièrement, les entreprises doivent fournir à des auditeurs externes la preuve de leur conformité à des contraintes réglementaires. Par celles-ci, la loi américaine Sarbanes-Oxley (SOX) affecte les entreprises américaines et d'une façon générale les sociétés cotées aux Etats-Unis.

Ces lois et règlements peuvent viser à préserver l'intégrité de données financières (cas de SOX et de la Loi sur la Sécurité Financière) ou médicales (règlement américain 21 CFR Part 11), la confidentialité des données personnelles etc.

Le rôle des preuves dans la certification

D'une manière générale, la conformité exige d'identifier des **risques**, décider d'**objectifs** de contrôle pour y faire face et mettre en place des **activités** de contrôle pour parvenir à ces objectifs. Enfin, face à ces activités, il convient de préparer les **tests** adéquats pour s'assurer que ces processus existent, sont appliqués et fonctionnent efficacement.

La finalité de ces tests est double. D'une part, ils permettent d'améliorer en permanence les processus et d'informer le management et les auditeurs internes. D'autre part, ces tests seront utilisés comme **preuves** lors de la certification pour convaincre les auditeurs externes de conformité de l'organisation.

Gérer les identités et les accès

Sur le terrain, on constate qu'une grande partie des risques de non-conformité à ces textes provient d'une gestion inadéquate des identités et des accès. En effet, au-delà du vol d'identité, des actions rendues possibles par des droits d'accès mal attribués sont une source majeure de brèches de sécurité.

Par conséquent, une solution de **gestion des identités et des accès** (en anglais Identity and Access Management ou IAM) peut apporter une aide significative dans l'effort de mise en conformité à ces lois et règlements. De même, une telle solution permet de mettre à jour simplement un ensemble existant de procédures de contrôle afin de la simplifier ou de l'adapter aux changements d'organisation.

Quel reporting pour la gestion des identités et des accès ?

Outre les fonctions qu'elle apporte, la gestion des identités et des accès doit donc apporter la preuve de son bon fonctionnement. Ces preuves devront être fournies sur demande à un auditeur sous forme de trace écrite, afin d'être archivées.

Quels rapports demander à un fournisseur de solution de gestion des identités et des accès ? Clairement, les rapports fournis ne doivent pas être figés : la plupart des lois et règlements ne spécifient évidemment pas le format des informations. Chaque rapport est généré pour couvrir une situation d'entreprise particulière, et être consulté par des auditeurs internes et externes. Les informations fournies doivent donc être :

- Adaptables, afin d'être utilisées pour des situations diverses
- Vérifiables pour que l'auditeur puisse s'assurer de l'exactitude des données
- Fidèles, pour représenter la réalité des données

Et bien entendu, les rapports doivent couvrir les zones les plus fréquemment concernées par les exigences des lois et réglementations.

La gestion raisonnée des identités et des accès

Avec des milliers d'utilisateurs et des centaines de ressources de tous types, la gestion des identités et des accès peut facilement devenir ingérable. Pour éviter cela, il est très utile de mettre en place une méthode de gestion raisonnée des accès.

Gérer de façon centralisée les identités et les accès présente des avantages indéniables en termes de conformité. Lors de l'audit, la preuve est en effet facilitée car on dispose à un endroit unique des données d'accès. Mais surtout, cela permet d'adopter une méthodologie cohérente de gestion, sous le contrôle de la politique de sécurité de l'entreprise.

Par exemple, Evidian recommande de gérer de façon séparée les données concernant d'une part le **rôle** des personnes dans l'organisation (dites données « autoritatives »), d'autre part la **politique** des accès basée sur les rôles, et enfin les **autorisation** d'accès qui en sont déduites (données « attribuées »).

Cette méthode de gestion offre de nombreux avantages, par exemple :

- Séparer les rôles d'administrateurs entre gestionnaires de personnes et gestionnaires de politique d'accès.
- Assigner tous les droits d'accès en fonction de la fonction de l'utilisateur, et donc de son rôle dans l'entreprise.
- Rendre cohérents les rapports sur les attributions des droits d'accès, et donc faciliter les audits ultérieurs.

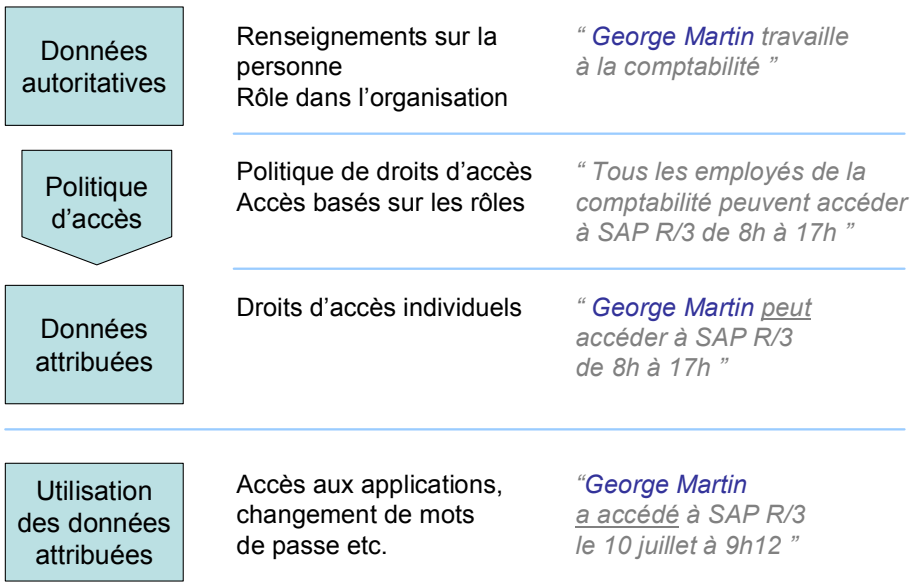
Données autoritatives
Renseignements sur la personne
Rôle dans l'organisation
" George Martin travaille à la comptabilité "
Politique d'accès
Politique de droits d'accès
Accès basés sur les rôles
" Tous les employés de la comptabilité peuvent accéder à SAP R/3 de 8h à 17h "
Données attribuées
Droits d'accès individuels
" George Martin peut accéder à SAP R/3 de 8h à 17h "
Utilisation des données attribuées
Accès aux applications, changement de mots de passe etc.
"George Martin a accédé à SAP R/3 le 10 juillet à 9h12 "

Figure 1 : Gestion raisonnée des identités et des accès

Avec une gestion rationnelle des identités et des accès, les rapports d'audit peuvent en effet documenter des sous-ensembles cohérents de l'activité de gestion des accès :

- Rapports sur le cycle de vie des identités et des rôles
- Rapports sur le cycle de vie de la politique d'accès
- Rapports de non-conformité sur les droits d'accès
- Rapports sur le comportement des utilisateurs

Cadre de référence de la loi Sarbanes-Oxley

L'article 404 de la loi Sarbanes-Oxley ne stipule pas quel ensemble de catégories formelles d'évaluation, appelé « framework », doit être observé pour évaluer les contrôles de la production des rapports financiers. De même, les règles définitives de la SEC (Securities and Exchange Commission), indiquent spécifiquement qu'elles *"ne précisent pas la méthode ou les procédures à appliquer lors d'une évaluation".*

Cependant, les règles de la SEC citent précisément le cadre du Committee of Sponsoring Organizations (COSO), bien que des cadres régionaux de contrôle d'entreprise puissent être utilisés. De même, des cadres spécifiques de contrôle du SI peuvent être choisis par une entreprise, du moment que l'entreprise en question peut convaincre son auditeur externe que ses contrôles répondent aux exigences d'efficacité.

Un cadre d'objectifs de contrôle du SI souvent utilisé dans le contexte de SOX est le Control Objectives for Information and related Technology - COBIT, émis par le IT Governance institute – ITGI (www.itgi.org).

La loi Sarbanes-Oxley a créé le Public Company Accounting Oversight Board (PCAOB), organisation à but non lucratif visant à contrôler les commissaires aux comptes des sociétés. Le PCAOB est chargé de définir des directives destinées aux auditeurs, sur la façon dont ils doivent auditer les différents aspects de l'organisation, notamment ceux relatifs à l'article 404 de la loi.

Du moment que les contrôles en résultant satisfont aux exigences définies par les normes d'audit du PCAOB, il est concevable que des sociétés s'appuient sur d'autres cadres de contrôle du SI que le COBIT. Lesdits cadres peuvent s'appuyer sur ITIL (IT Infrastructure Library - www.itil.co.uk) ou sur ISO 17799. Les sociétés peuvent également choisir un cadre de contrôle des comptes mis au point par les entreprises de conseil et d'audit.

Il est donc important que les sociétés travaillent en étroite collaboration avec leurs auditeurs externes, tout particulièrement pendant les premières phases d'application et de certification de l'article 404 de la loi Sarbanes-Oxley.

Pour de plus amples informations sur ce sujet, veuillez vous reporter au livre blanc d'Evidian « Sarbanes-Oxley and Identity and Access Management » (« Sarbanes-Oxley et la gestion des identités et des accès ») :

http://www.evidian.com/p/am.php?d=wpsox&c=rep

Constitution de votre dossier pour vos auditeurs

Détermination des contrôles : le cycle de vie SOX

Lors de l'audit des comptes d'une entreprise soumise à Sarbanes-Oxley, les commissaires aux comptes doivent vérifier si les contrôles mis en place :

- existent, sont appropriés et documentés
- sont appliqués à tous les niveaux
- produisent les effets escomptés

Les preuves de la bonne exécution des contrôles doivent être fournies sur demande aux auditeurs. La manière de les obtenir doit donc être elle-même documentée.

Ces preuves – qui sont souvent des rapports d'exécution ou des historiques – seront d'autant plus convaincantes si elles sont elles-mêmes régulièrement utilisées en interne. Pour faire évoluer régulièrement un ensemble de contrôles Sarbanes-Oxley, il faut en effet être capable d'en évaluer l'efficacité.

L'effort de conformité à Sarbanes-Oxley n'est en effet pas un effort unique, réalisé une fois pour toutes. Les contrôles doivent pouvoir évoluer, d'une part parce que l'organisation évolue, d'autre part pour optimiser leur efficacité et leur coût. L'entreprise doit donc établir un cycle de vie SOX, au cours duquel les contrôles sont régulièrement évalués.

Dans le cas particulier de la gestion des identités et des accès, la gestion centralisée des utilisateurs et de la politique de sécurité peut permettre de faciliter le cycle de vie SOX :

- Production de rapports mesurant l'efficacité des contrôles
- Gestion centralisée facilitant la mise en place des contrôles
- Mise en place rapide des nouvelles décisions concernant la politique de sécurité

Que doit fournir un rapport sur la sécurité ?

Données exactes et non altérées

Un rapport fourni à un auditeur doit être le reflet le plus fidèle possible de la réalité. Pour cela, il est nécessaire de produire les données telles qu'elles sont conservées dans les bases de sécurité. Si un outil réalise de façon intempestive des « déductions » et corrections de données avant de les publier, les résultats risquent de ne pas être acceptés faute d'éléments probants.

A l'inverse, si l'outil produit des données dignes de confiance, un auditeur les acceptera comme éléments de preuve, et n'exigera pas des données complémentaires provenant d'autres sources.

Un outil de gestion des identités et des accès doit donc documenter l'origine des données qu'il fournit et assurer, dans sa documentation, que les données ne sont pas modifiées lors de la production de rapports.

Reporting complet

Un environnement de reporting doit pouvoir couvrir un ensemble d'informations aussi complet que possible. L'objectif n'est bien sûr pas de fournir une quantité massive d'information lors de l'audit, mais d'être capable de produire des données les plus complètes sur les domaines spécifiques qui ont été choisis.

Les données fournies doivent donc couvrir les domaines fréquemment couverts par les audits, notamment :

- Activité des administrateurs
- Activité des utilisateurs finaux
- Tests de conformité avec la politique de sécurité

Outre ces thèmes généraux, les données doivent être suffisamment détaillées. Par exemple, il sera difficile d'évaluer la conformité à la politique de gestion de mots de passe si les informations fournies ne comportent pas la date de dernier changement de mot de passe.

Reporting adaptable

Les rapports générés pour Sarbanes-Oxley ont un but précis : permettre de démontrer aux auditeurs que les contrôles mis en place sont opérationnels et efficaces. Ils doivent donc être ciblés et comporter précisément l'information nécessaire, sans surplus de données.

Les situations variant de façon notable suivant les entreprises, il est donc particulièrement critique de disposer d'un environnement de reporting adaptable. Des rapports pré-packagés risquent d'être, soit insuffisants, soit trop copieux pour démontrer un point précis de façon convaincante.

Il est donc particulièrement utile de s'assurer du caractère adaptable des données de reporting fournies par un outil de gestion des identités et des accès.

Cela concerne notamment à la fois le type d'information fourni (par exemple dernier accès à l'application, rôle de l'utilisateur etc.) et le domaine concerné (uniquement les financiers de Boston, uniquement les accès à SAP R/3 etc.)

Par ailleurs, il peut être efficace de produire les rapports finaux en s'appuyant sur les outils standards de l'entreprise (notamment *BusinessObjects*™ ou *Crystal Reports*™). En effet :

- Les compétences en outils de « business intelligence » sont souvent localisées dans les mêmes équipes financières qui sont en contact avec les auditeurs.

- Les rapports sur la gestion des identités et des accès ne sont qu'un des multiples types de rapports générés lors d'un audit soumis à Sarbanes-Oxley. Il n'est donc pas efficace de devoir exécuter simultanément de nombreux outils de reporting, chacun spécifique à un domaine donné, au cours d'un audit.

La tâche de l'outil de gestion des identités et des accès sera alors de produire les données brutes sous un format compatible (CSV par exemple), tandis que les rapports seront préparés en utilisant les compétences internes.

Environnement de production de rapports

Lors d'un audit, il faut produire des données sur de nombreux autres sujets que la gestion des accès.

La valeur ajoutée de l'outil de gestion des identités et des accès est de fournir des données sur l'activité des administrateurs et des utilisateurs, ainsi que sur la cohérence des droits d'accès avec la politique de sécurité de l'entreprise.

Par ailleurs, d'autres sources d'information fourniront les preuves de bon fonctionnement des contrôles concernant d'autres domaines que la gestion des identités et des accès. Notamment les logiciels de comptabilité, les outils de reprise sur sinistre etc.

Pour bien gérer toutes ces sources d'information, il peut être utile de les compléter par des outils annexes :

- *Logiciel d'ordonnancement* afin de déclencher la production en temps voulu des données destinées à de futurs audits,
- *Service d'archivage* (avec valeur légale ou non) pour conserver la trace de ces données.
- *Business intelligence* pour produire de façon facile et reproductible des rapports clairs et lisibles.

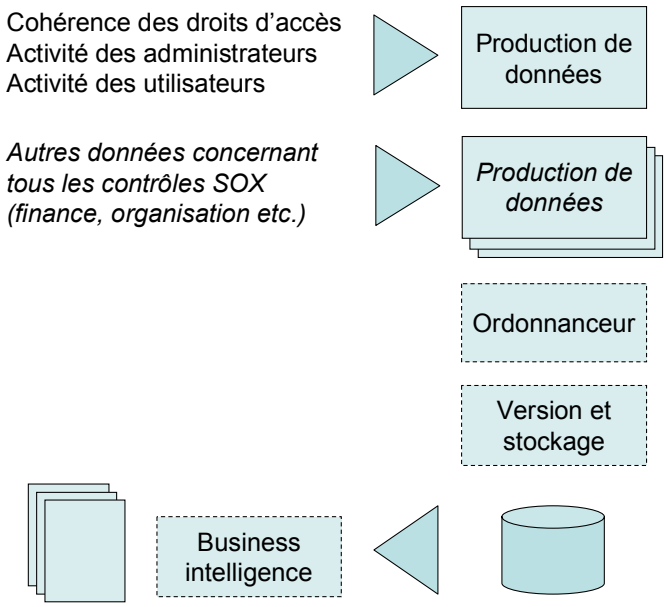

Figure 2 : Environnement de production de rapports d'audits

Notez que l'utilisation des outils annexes n'est nullement obligatoire dans tous les cas. Pour certains contrôles, le commissaire aux comptes pourra simplement demander un état à la date de l'audit : la chaîne d'ordonnancement et d'archivage ne sera pas utile dans ces cas-là.

Vérifiabilité

Vos rapports d'audit peuvent-ils être eux-mêmes audités ?

Pour qu'un auditeur accepte un document comme preuve du bon fonctionnement d'un processus, il doit pouvoir s'assurer que l'information contenue n'a pas été altérée.

Dans ce but, les informations contenues dans les rapports doivent être vérifiables. Un auditeur doit pouvoir demander de confirmer un échantillon de rapport par un autre moyen d'investigation.

Ce moyen peut être une confirmation par un autre outil de diagnostic, mais aussi la consultation des bases de données par une console d'administration. Dans tous les cas, il peut être utile de fournir un mode d'emploi lors de l'audit.

Rapport par actions ou par état

Un principe de la comptabilité en partie double est qu'à un instant donné, le résultat financier du **bilan** est le même que celui du **compte de résultat**. Cependant, en fonction du type d'information à vérifier, il peut faire plus de sens pour un auditeur d'exiger des preuves relevant du bilan (solde de comptes en banque par exemple) ou du compte de résultat (factures par exemple).

Un parallèle peut être fait avec la gestion des identités et des droits d'accès.

Selon le contrôle dont un auditeur vérifie l'efficacité, il pourra exiger un **état actuel** sur les ressources et les utilisateurs, ou demander une **liste des actions** précise ayant abouti à cet état.

Pour remplir ces demandes, l'outil de gestion des identités et des accès doit pouvoir fournir les deux types de vues.

Rapports sur état actuel		**Rapports sur actions pendant une période de temps**
Liste des droits d'accès	⇔	Actions d'attribution, modifications et suppressions des droits d'accès
Liste des comptes bloqués	⇔	Accès des utilisateurs à des ressources
Liste des groupes d'utilisateurs	⇔	Créations, modifications et suppressions des groupes d'utilisateurs.
« Age » des mots de passe d'une catégorie d'utilisateurs	⇔	Actions de changement de mots de passe

Tableau 1 : Exemples de types de rapports

Exemple de chaînes SOX – risque, contrôle et test

Dans cette section, nous vous donnons des exemples de chaînes concernant des contrôles et la **production des rapports** correspondants dans le domaine de la gestion des identités et des accès.

Ces rapports sont conçus pour tester les **activités de contrôle**, qui sont elles-mêmes établies pour atteindre les **objectifs de contrôle**. Enfin, ces objectifs sont censés réduire sensiblement des **risques** précis, qui auraient pu être détectés durant les audits précédents.

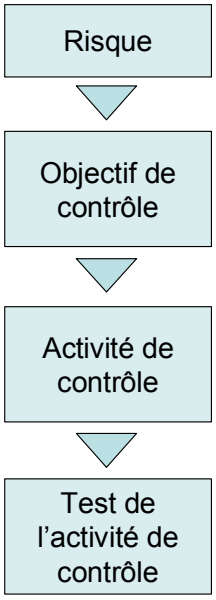

Figure 3 : Partir des risques pour déterminer les activités de contrôle et tests

Veuillez bien noter que ce ne sont que des *exemples*, car aucune série de contrôles ne peut être adoptée en bloc par une société. Cela serait contraire au but des contrôles SOX, c'est-à-dire assurer qu'une entreprise a pris les mesures nécessaires à la réduction de risques qui lui sont propres concernant l'intégrité de ses rapports financiers. Les risques sont propres à chaque société, il en est donc de même pour les mesures correctrices.

Cependant, la liste suivante peut vous donner une idée du rôle que peut jouer un outil de gestion des identités et des accès pour faciliter les audits dans le cadre de SOX, tout particulièrement concernant l'article 404 de la loi. De même, cette liste ne constitue pas une énumération exhaustive de tous les contrôles possibles.

Terme	Explication
Unité Organisationnelle	Partition administrative de l'annuaire d'une société. Certains outils de gestion des identités et des accès peuvent utiliser l'annuaire LDAP de l'entreprise comme source d'information sur les utilisateurs. Cela rend ainsi inutile toute duplication des données ou tout effort supplémentaire d'administration des utilisateurs.
Solution de provisionnement	Solution créée pour aider les administrateurs à attribuer efficacement les ressources et les privilèges aux utilisateurs. Les activités de provisionnement doivent être effectuées selon des règles correspondant à la politique de sécurité de la société.
Recommandation (« guidance ») de l'ITGI	Contrôle illustratif figurant dans le document "*IT Control Objectives for Sarbanes-Oxley*" émis par l'ITGI en avril 2004. Ce document dresse la liste des sujets susceptibles d'être traités si le processus général de mise en conformité à Sarbanes-Oxley a été effectué en suivant le modèle du COBIT.
Groupe d'utilisateurs	Regroupement administratif d'utilisateurs. C'est une manière courante d'attribuer *des rôles* aux utilisateurs et de leur attribuer des ressources en se fondant sur ces rôles. Le terme « profil » peut également être utilisé au lieu de « groupe d'utilisateurs ». Un utilisateur peut être membre de plusieurs groupes d'utilisateurs.
Auto-inscription	Technique de déploiement de l'authentification unique (SSO). Pendant le déploiement, l'inscription d'un utilisateur à une application n'est terminée que si l'utilisateur lance réellement l'application et donne son identité et son mot de passe actuel.

Tableau 2 : Quelques termes utilisés dans cette section

Les contrôles spécifiques à la gestion des identités et des accès sont mis en pratique avec la solution Evidian AccessMaster.

Pour de plus amples informations sur le choix d'une gestion des identités et des accès afin de faciliter la conformité à Sarbanes-Oxley, veuillez vous reporter au livre blanc ci-dessous :

http://www.evidian.com/p/am.php?d=wpsox&c=rep

Politique de sécurité du SI

Cycle de vie de la politique de sécurité

Domaine	Contenu
Modèle de l'ITGI	*« Le plan de sécurité du SI est mis à jour pour refléter les changements dans l'environnement du SI, ainsi que les exigences de sécurité de systèmes spécifiques. »*
Exemple de risque	Des changements du plan de sécurité du SI concernant les groupes d'utilisateurs pourraient ne pas être reportés dans les outils de sécurité du SI.
Objectif de contrôle	Utiliser strictement les groupes d'utilisateurs définis dans le plan de sécurité du SI.
Exemple d'activité de contrôle	Tous les profils créés dans le système de SSO doivent correspondre aux profils définis dans le document sur la politique de sécurité du SI.
Exemple de test d'activité de contrôle	Demander la liste des groupes d'utilisateurs gérés par le système de SSO. Vérifier qu'ils correspondent aux groupes d'utilisateurs définis dans le plan de sécurité du SI.

Exemple de rapport pour l'activité de contrôle :

R06b **Rapport créé le 15 juin 2012**
Filtre : UO = "Finance"

Groupe d'utilisateurs	Nombre d'utilisateurs qui appartiennent au groupe d'utilisateurs
(None)	5
Secrétaires	12
Gestion de comptes clients	20
Gestion de comptes fournisseurs	19
Saisie de données	8
Recouvrement	6

Authentification de l'utilisateur

Déployer une authentification unique dans toute l'entreprise

Domaine	Contenu
Modèle de l'ITGI	*« Des procédures existent et sont suivies pour authentifier tous les utilisateurs dans le système afin d'assurer la validité des transactions ».*
Exemple de risque	Attribuer de multiples mots de passe aux utilisateurs peut les inciter à partager leurs mots de passe, à les perdre ou à les noter sur un support papier ou électronique.
Objectif de contrôle	Authentification unique (SSO)
Exemple d'activité de contrôle	Les utilisateurs sont inscrits dans (et accèdent à leur application par) un environnement d'authentification unique.
Exemple de test d'activité de contrôle	Demander la liste des utilisateurs appartenant à une UO donnée. Vérifier s'ils sont actifs dans l'environnement d'authentification unique (regardez la dernière connexion et surlignez si elle date de plus de NN jours). Vérifiez si cette liste correspond aux utilisateurs attendus en vérifiant sur la liste des RH.

Exemple de rapport pour l'activité de contrôle :

R01 **Rapport créé le 15 juin 2012**

Filtre : UO = "Finance"
Filtre : Groupes d'utilisateurs = "Consolidation

Identification unique	Prénom	Nom	UO	Groupe d'utilis.	Dernière connexion
MICHAEL_ALVAREZ	Michael	Alvarez	Finance	Consolidation	12/06/2012
BARBARA_GRIFFIN	Barbara	Griffin	Finance	Consolidation	12/06/2012
SARAH_JORDAN	Sarah	Jordan	Finance	Consolidation	12/06/2012
JANE_LOGAN	Jane	Logan	Finance	Consolidation	01/06/2012
PAUL_MORTON	Paul	Morton	Finance	Consolidation	02/06/2012
MARK_SMITH	Mark	Smith	Finance	Consolidation	12/06/2012
JOHN_WALKER	John	Walker	Finance	Consolidation	12/06/2012

Domaine	Contenu
Exemple de risque	Les mots de passe faciles à deviner réduisent la sécurité
Objectif de contrôle	Politique forte des mots de passe primaires
Exemple d'activité de contrôle	Un format de mot de passe fort est appliqué pour le nom d'utilisateur primaire et pour les applications
Exemple de test d'activité de contrôle	Demander les formats appliqués pour le nom d'utilisateur primaire (et l'identifiant utilisé pour l'application si le système d'authentification unique gère le changement de mot de passe)

Forcer l'expiration du mot de passe

Domaine	Contenu
Modèle de l'ITGI	*« Des procédures existent et sont appliquées pour maintenir l'efficacité de l'authentification et des mécanismes d'accès (par exemple des changements réguliers de mot de passe). »*
Exemple de risque	Si les mots de passe ne sont pas changés régulièrement, la probabilité augmente qu'un mot de passe soit volé puis utilisé plus tard.
Objectif de contrôle	Expiration du mot de passe
Exemple d'activité de contrôle	L'expiration du mot de passe (45 jours) est appliquée pour l'authentification primaire.
Exemple de test d'activité de contrôle	Demander la liste des utilisateurs dont le mot de passe primaire date de plus de 45 jours. Vérifier que ces utilisateurs n'ont pas réussi à se connecter après la date d'expiration à respecter.

Exemple de rapport pour l'activité de contrôle :

R03 **Rapport créé le 15 juin 2012**

Filtre : Dernier changement général de mot de passe < 03/03/2012

Identification unique	Prénom	Nom	UO	Groupe d'utilisateurs	Dernière connexion	Dernier changement général de mot de passe	Etat actuel
BARBARA_LOGAN	Barbara	Logan	Finance	Comptes clients	03/03/2012	02/02/2012	Actif
MICHAEL_SMITH	Michael	Smith	Finance	Consolidation	10/12/2011	10/12/2011	Bloqué
JANE_WALKER	Jane	Walker	Finance	Secrétaires	10/06/2012	01/01/2012	Actif

Gestion des autorisations d'accès de l'utilisateur

Suppression des comptes inactifs

Domaine	Contenu
Modèle de l'ITGI	*« Des procédures existent et sont appliquées pour assurer une action rapide concernant la demande, l'établissement, l'émission, la suspension et la fermeture des comptes d'utilisateur. »*
Exemple de risque	Les utilisateurs qui ne sont plus actifs (longue maladie, etc.) ont des comptes inactifs qui pourraient être exploités.
Objectif de contrôle	Retirer régulièrement les utilisateurs inactifs.
Exemple d'activité de contrôle	Lorsqu'un utilisateur n'a pas utilisé son poste de travail depuis 90 jours, il doit être désactivé et/ou retiré de la base dans un délai de 2 semaines.
Exemple de test d'activité de contrôle	Demander la liste des membres du groupe d'utilisateurs « Comptabilité » qui n'ont pas utilisé leur poste de travail depuis 90 jours.

Exemple de rapport pour l'activité de contrôle :

R05 **Rapport créé le 15 juin 2012**

Filtre : Dernière utilisation du poste de travail < 03/03/2012

Identification unique	Prénom	Nom	UO	Groupe d'utilisateurs	Dernier changement général de mot de passe	Etat actuel
JANE_WALKER	Jane	Walker	Finance	Secrétaires	01/01/2012	Actif
MICHAEL_SMITH	Michael	Smith	Finance	Consolidation	10/12/2011	Bloqué
BARBARA_LOGAN	Barbara	Logan	Finance	Comptes clients	02/02/2012	Actif

Autorisations d'accès octroyées selon le profil

Domaine	Contenu
Modèle de l'ITGI	*« Un processus de contrôle existe et est suivi de façon à réviser et confirmer régulièrement les autorisations d'accès. »*
Exemple de risque	Les autorisations d'accès pourraient être octroyées individuellement, en dehors de la politique de la société, créant des brèches de sécurité.
Objectif de contrôle	Autorisations d'accès octroyées seulement en fonction du profil.
Exemple d'activité de contrôle	Toutes les inscriptions aux ressources doivent résulter de l'appartenance d'un utilisateur à un profil. Aucune inscription directe d'un utilisateur à une ressource ne doit être effectuée.
Exemple de test d'activité de contrôle	Demander la liste des inscriptions n'ayant pas été attribuées selon un profil.

Exemple de rapport pour l'activité de contrôle :

R07 **Rapport créé le 15 juin 2012**

Identification unique	Prénom	Nom	UO	Groupe d'utilisateurs	Ressource	Rôle de l'utilisateur	Inscription créée le
ALEXANDRA_LOGAN	Alexandra	Logan	Finance	Audit Interne	SAP R/3	Utilisateur	02/02/2012
JANE_MARTIN	Jane	Martin	Finance	Comptes clients	SAP R/3	Administrateur	03/04/2012
JAMES_JONES	James	Jones	Finance	Secrétaires	Intranet	Utilisateur	01/05/2012
JOHN_ALVAREZ	John	Alvarez	Finance	Comptes clients	SAP HR	Utilisateur	12/06/2012

Auto-inscription

Domaine	Contenu
Exemple de risque	L'accès à l'application pourrait être octroyé par erreur à des utilisateurs n'ayant pas besoin de cet accès dans l'exercice de leurs fonctions.
Objectif de contrôle	Les groupes d'utilisateurs doivent être conçus pour fournir l'accès aux applications par les utilisateurs qui ont réellement besoin de l'accès.
Exemple d'activité de contrôle	Mettre des applications spécifiques en mode d'auto-inscription. Quelques temps après, regarder quels utilisateurs se sont réellement inscrits. Les définitions des groupes d'utilisateurs devraient être révisées si des utilisateurs n'utilisent en fait pas l'application.
Exemple de test d'activité de contrôle	Pour les applications nécessitant une auto-inscription, demander la liste des utilisateurs ayant réellement effectué une auto-inscription. La comparer à la liste des utilisateurs censés utiliser l'application.

Exemple de rapport pour l'activité de contrôle :

R13 **Rapport créé le 15 juin 2012**

Filtre : Ressource = "Comptabilité générale"
Filtre : UO = "Finance"
Filtre : Groupe d'utilisateurs = "Comptes clients"

Identification unique	Prénom	Nom	UO	Groupe d'utilisateurs	Ressource	Date d'auto-inscription
GEORGE_MARTIN	George	Martin	Finance	Comptes clients	Compta générale	13/06/2012
MICHAEL_JONES	Michael	Jones	Finance	Comptes clients	Compta générale	13/06/2012
BARBARA_LOGAN	Barbara	Logan	Finance	Comptes clients	Compta générale	14/06/2012
MICHAEL_SMITH	Michael	Smith	Finance	Comptes clients	Compta générale	N/A
BARBARA_LOGAN	Barbara	Logan	Finance	Comptes clients	Compta générale	N/A

Reporting sur les incidents de sécurité

Domaine	Contenu
Modèle de l'ITGI	*« L'administration de la sécurité du SI surveille et enregistre l'activité, et les violations de la sécurité identifiées sont signalées à la hiérarchie supérieure. »*
Exemple de risque	L'utilisateur pourrait essayer différents mots de passe successivement sur le poste de travail d'un autre utilisateur, obtenant ainsi l'accès.
Objectif de contrôle	Bloquer l'accès après 10 tentatives infructueuses, signaler cela à la direction.
Exemple d'activité de contrôle	Après 10 authentifications originales infructueuses, l'utilisateur doit être automatiquement bloqué dans toute autre tentative d'authentification, et un rapport des dits incidents doit être envoyé à la direction. Des tests mensuels doivent être réalisés en saisissant intentionnellement des mots de passe incorrects sur un poste de travail de test.
Exemple de test d'activité de contrôle	Demander la liste des évènements *« utilisateur bloqué à la suite de 10 authentifications infructueuses »* sur une période donnée. Vérifier que les tests mensuels ont été réalisés.

Exemple de rapport pour l'activité de contrôle :

R10 **Rapport créé le 15 juin 2012**

Filtre : Saisir date entre le 01/01/2012 et le 15/01/2012
Filtre : Saisir type ="Trop d'authentifications infructueuses"

Identification unique	Prénom	Nom	UO	Profil	Date de saisie
GEORGE_WALKER	George	Walker	Finance	Secrétaires	03/01/2012
MICHAEL_BUSH	Michael	Bush	Finance	Comptes clients	05/01/2012
BARBARA_LOGAN	Barbara	Logan	Finance	Secrétaires	13/01/2012

Eliminer les comptes par défaut

Domaine	Contenu
Exemple de risque	Les comptes pourraient être créés par les administrateurs (ou il se pourrait que des comptes par défaut existent) en dehors de la politique de sécurité.
Objectif de contrôle	Détecter et éliminer les comptes existant en dehors de la politique de sécurité.
Exemple d'activité de contrôle	Attribuer toutes les autorisations d'accès avec un outil de provisionnement. Retirer les comptes par défaut.
Exemple de test d'activité de contrôle	Concernant les ressources sensibles, demander la liste des comptes qui sont présents dans le système d'information, mais qui ne correspondent à aucun utilisateur connu dans l'outil de provisionnement.

Exemple de rapport pour l'activité de contrôle :

R21 **Rapport créé le 15 juin 2012**
Filtre : Ressource = "SAP R/3"

Application ID utilisateur	Ressource
UTILISATEUR GENERIQUE	SAP R/3
TEST	SAP R/3
MARTIN-R	SAP R/3
A COMPLETER	SAP R/3

Cloisonnement des tâches

Exemple

Domaine	Contenu
Modèle de l'ITGI	*« Des contrôles relatifs au cloisonnement approprié des tâches concernant la demande et l'attribution de l'accès aux systèmes et données existent et sont respectés. »*
Exemple de risque	Les administrateurs de la sécurité pourraient attribuer des autorisations d'accès à des applications ne faisant pas partie de leurs responsabilités.
Objectif de contrôle	Restreindre les droits des administrateurs selon le profil.
Exemple d'activité de contrôle	Définir les profils de l'administrateur, et octroyer restrictivement à ces profils le droit de donner des autorisations d'accès aux applications.
Exemple de test d'activité de contrôle	Pour un profil d'administrateur spécifique, demander la liste des actions d'administration par les membres de ce profil sur une période donnée. Vérifier que ces actions ne concernaient que des applications autorisées.

Exemple de rapport pour l'activité de contrôle :

R21 Filtre : Action ="Inscrit"			Rapport créé le 15 juin 2012			
Identification unique	**Prénom**	**Nom**	**Ressource**	**Groupe de Ressources**	**Créé**	**Dernière connexion**
MICHAEL_MARTIN	Michael	Martin	SAP HR	Finance_app	01/01/2010	12/06/2012
SARAH_GRIFFIN	Sarah	Griffin	SAP HR	Finance_app	01/01/2010	12/06/2012
CLARA_JORDAN	Clara	Jordan	SAP R/3	Finance_app	03/05/2011	12/06/2012
ALBERTO_GEORGE	Alberto	George	SAP R/3	Finance_app	03/05/2011	13/06/2012

Preuve d'accès aux ressources

Enregistrement des accès aux applications

Domaine	Contenu
Modèle de l'ITGI	*« Le cas échéant, des contrôles existent pour assurer qu'aucune partie ne puisse nier des transactions, et des contrôles sont réalisés pour produire une non-répudiation d'origine ou de réception, preuve de dépôt et de réception de transactions. »*
Exemple de risque	Un utilisateur pourrait nier avoir accédé à une application spécifique.
Objectif de contrôle	Enregistrement des accès aux applications
Exemple d'activité de contrôle	Les accès aux applications individuelles doivent être enregistrés et l'historique des accès doit être stocké de façon centrale.
Exemple de test d'activité de contrôle	Demander la liste des accès à une application sensible spécifique sur une période donnée.

Exemple de rapport pour l'activité de contrôle :

R21 Filtre : Action ="Inscrit"			Rapport créé le 15 juin 2012			
Identification unique	**Prénom**	**Nom**	**Ressource**	**Groupe de Ressources**	**Créé**	**Dernière connexion**
MICHAEL_MARTIN	Michael	Martin	SAP HR	Finance_app	01/01/2010	12/06/2012
SARAH_GRIFFIN	Sarah	Griffin	SAP HR	Finance_app	01/01/2010	12/06/2012
CLARA_JORDAN	Clara	Jordan	SAP R/3	Finance_app	03/05/2011	12/06/2012
ALBERTO_GEORGE	Alberto	George	SAP R/3	Finance_app	03/05/2011	13/06/2012

For more information go to www.evidian.com/

Email: info@evidian.com